Notice to File Missing Parts on a timely basis with an adequate filing fee to pay for both the originally filed claims and the claims added in this Preliminary Amendment. Since the Applicants are unsure when the declarations will be executed, the Applicants will submit the filing fees, late declaration surcharge, and any extension of time fees when the declarations are executed.

If the OIPE Office is unable to enter this preliminary amendment into the file because of the lack of fees, the Applicants authorize the Assistant Commissioner and all related personnel to charge any necessary fees, or credit any overpayment, to Deposit Account 11-0980.

AMENDMENT

In the Claims

Please amend the following claims:

---

1. (Amended) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

A1

creating scope criteria for analyzing security event data;

collecting the security event data from a plurality of security devices located at a first location;

storing the collected security event data at a second location; and

analyzing the collected security event data with the scope criteria to produce result data, the result data accessible by a plurality of clients.

A2 Cmt

3. (Amended) The method of Claim 1, wherein the first location is a distributed computing environment and the second location is a database server.

A2 Cancel

4. (Amended) The method of Claim 1, wherein collecting the security event data comprises

generating security event data from a sensor;

sending the security event data from the sensor to a collector; and

converting the event data to a common format.

16. (Amended) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

creating scope criteria for filtering security event data;

A3

generating security event data from a plurality of security devices located at a first location;

collecting security event data at a second location; and

applying the scope criteria to the security event data at a third location to produce a result, the result accessible by a plurality of clients coupled to a server.

17. (Amended) The method of Claim 16, further comprising rendering the result in a rendering for output to a client.

20. (Amended) The method of Claim 16, wherein the third location is an application server coupled to the plurality of clients.

A4

21. (Amended) The method of Claim 16, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

22. (Amended) The method of Claim 16, further comprising executing an action at the server in response to producing the result.

A5

25. (Amended) The method of Claim 16, further comprising applying additional scope criteria to a plurality of results.

27. (Amended) A computer-implemented system for managing security event data collected from a plurality of security devices comprising:

a plurality of security devices operable for generating security event data;

an event manager coupled to the security devices, the event manager operable for collecting security event data from the security devices and analyzing the security event data; and

A6

a client coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager.

28. (Amended) The system of Claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data.

29. (Amended) The system of Claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response.

Please add the following new claims:

31. (New) The system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager.

A7
Cm.t

32. (New) The method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data.

33. (New) The method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients.

34. (New) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

creating scope criteria for analyzing security event data;

generating the security event data from a plurality of security devices located at a first location;

collecting the security event data at a second location;

analyzing the collected security event data with the scope criteria at a third location to produce result data, the result data accessible by a plurality of clients; and

rendering the result data in a manageable format for the plurality of clients.

35. (New) The method of Claim 34, further comprising storing one or more of the scope criteria, the security event data, and the result data.

A7
Cm 1+

36. (New) The method of Claim 34, wherein the first location is a distributed computing environment, the second location is a database server, and the third location is an application server to which the plurality of clients are coupled.

37. (New) The method of Claim 34, further comprising editing the scope criteria.

38. (New) The method of Claim 34, further comprising converting the collected security event data to a common format.

39. (New) The method of Claim 35, further comprising searching the stored security event data for additional information identifying a security event.

40. (New) The method of Claim 35, further comprising:

polling a database server for current stored security event data;

analyzing the current stored security event data to produce current result data; and

rendering the current result data.

41. (New) The method of Claim 34, further comprising polling for messages containing information about scope criteria, security event data, or result data.

42. (New) The method of Claim 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data.

43. (New) The method of Claim 34, wherein the step of rendering the result data comprises presenting the result data in a chart format.

A7 cm 4

44. (New) The method of Claim 34, wherein in response to analyzing the collected security event data, an action is executed.

45. (New) The method of Claim 44, wherein the action is clearing security event data from storage.

46. (New) The method of Claim 44, wherein the action is creating an incident from result data for preparing a response.

47. (New) The method of Claim 34, wherein the step of collecting security event data further comprises converting the data to a uniform format.

48. (New) A computer-readable medium having computer-executable instructions for performing the steps recited in claim 34.

49. (New) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

responsive to the plurality of security devices, generating security event data;

transferring the security event data from the security devices for storage in a database; and

applying a scope criteria to the security event data to produce a result by filtering the security event data, the result accessible by a plurality of clients coupled to an application server.

50. (New) The method of Claim 49, further comprising rendering the result in a rendering for output to the clients.

A7 Cont

51. (New) The method of Claim 49, further comprising the step of creating the scope criteria for filtering the security event data.

52. (New) The method of Claim 49, further comprising the step of editing the scope criteria.

53. (New) The method of Claim 49, further comprising converting the security event data to a uniform format.

54. (New) The method of Claim 49, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

55. (New) The method of Claim 49, wherein in response to producing a result, an action is executed.

56. (New) The method of Claim 55, wherein the action is clearing stored security event data.